The Success of the Deep Impact Mission

A Study of Risk Management Processes

Rick Grammier - Project Manager

Agenda

- State of the Project one year prior to launch
- Contributing causes for this state
- Solutions implemented
- Risk Management in context of solutions
- State of the Project at Launch
- Managing the risks for Encounter
- Summary

State of the Project One Year Prior to Launch (January 2004)

- Already had delayed launch one year (very unusual for a planetary launch)
- Had not completed development of the flight avionics hardware or software
- System level verification and validation program not started
- Fractured team and split responsibilities
- Science instruments completed and delivered
- Serious financial overruns - - NASA HQ on the verge of canceling the program

Contributing Causes for State of Affairs

- Rigorous engineering processes either not understood or not followed
  - Cultural differences between JPL and System Contractor
  - Knowledge and experience gaps within the team
  - Independent check and balance process eviscerated
- Reporting process did not provide a clear, overall picture
  - What are the primary issues and threats?
  - What are the plans and approaches for dealing with them?
  - What trends are being seen and what do they mean for the future?
- Ineffective Reviews Process
  - Only going through the motions, no real review rigor and penetration
  - Lack of rigorous follow-up and closure of issues uncovered
- Disorganized and ineffective teaming arrangements
  - Who has product responsibility at each level and at each life cycle phase?
  - Organization with the responsibility didn't necessarily have the knowledge or skills to deliver the product
  - Lack of effective management and leadership at multiple levels

Contributing Causes for State of Affairs - 2

- Lack of understanding and capability to conduct a flight system Validation and Verification (V&V) program
  - Two key V&V processes not implemented
  - Lack of understanding the “Verification” part of V&V
  - Need for very high fidelity test beds
  - No appreciation for data reduction and analysis needs
  - Late system maturation impeded scenario development and test
- Inadequate Flight Operations Concept and Plan
  - Lack of sufficient early staffing and funds
  - Very green team
  - Originally, the system contractor had responsibility
    - Significant experience and cultural mismatch
  - No appreciation for true impact of 1 year launch delay and only 6 months of operations

Solutions - Rigorous Engineering Processes

- JPL's Flight Project Practices and Design Principles
  - Team/Project had previously reviewed, but in piecemeal fashion
    - Lack of understanding in context of Deep Impact implementation
    - The **real value is in the discussion** of whether each requirement is met or not
  - Held several working meetings to go over each requirement
  - Exceptions are OK, but always **understand the risk** of each exception and the rationale as to why that risk is acceptable
    - New risks captured and tracked in the Project's Risk List
- Re-established Mission Assurance rigor
  - Formed a Mission Assurance Audit Team to determine state of affairs and make recommendations
  - Subsequently formed Tiger Team of experts to implement recommendations and correct deficiencies
  - It was painful and costly, but **- - - you have to do the right thing, right**

Example of Flight Project Practices

5.17	**Risk Management**
5.17.1	Risk management is conducted on all flight projects throughout the project life-cycle. Risks are considered in project cost estimation in the planning activities. Risk management includes consideration of risks related to cost, schedule, technical, scope, and mission success during the implementation of the project.
5.17.2	Each project prepares a Risk Management Plan, which documents the risk management objectives and approach over the project life cycle.
5.17.3	Each project prepares a Preliminary Risk Management Plan prior to PMSR, which is used during the project formulation phase.
5.17.4	Risk Management encompasses all elements of the project. When partners and /or system contractors are involved, they are essential participants in the Risk Management activity.
5.17.5	The project manager: Approves the final version of the Risk Management Plan prior to the PDR. Ensures that risks are identified and assessed using a standardized methodology, with pre-defined criteria for assessing likelihood and consequence of occurrence and approach to estimating total project risk. Ensures that risk to mission success (mission risk) and risk to implementation within program constraints (implementation risk) are assessed for each risk event identified. Takes appropriate actions based on the assessments to mitigate or retire risks. Alternatively, the project manager may elect to take no action, effectively accepting the risk without mitigation. Reports risks and risk status at each major review and at the *Governing Program Management Council* (GPMC) reviews. Presents and assesses risks and risk status in detail at the Mission Readiness Review. The results are used in support of JPLÕs recommendations to the cognizant NASA Enterprise Associate Administrator.
5.17.6	Projects review their Primary Risks (those risks having both high probability and high impact/severity) with the GPMC.
5.17.7	Projects manage risk using a JPL-developed, tailorable process (as described in Risk Management Handbook for JPL Projects) consistent with NASA Continuous Risk Management methodology. The project risk management process is documented in the Risk Management Plan. Risks are assessed according to pre-defined criteria as to their likelihood of occurrence, and consequence if they were to occur. Projects use and maintain a Significant Risk List.
5.18	**Waivers**
5.18.1	**Flight Project Practices** -- Projects needing to deviate from the requirements stated in the Practices sections of this document require waivers approved by the cognizant director-for.
5.18.1.1	Projects indicate planned compliance and non-compliance to the requirements through the use of the *FPP Compliance Matrix* . (preliminary at the PMSR and final at the PDR).

Example of Design Principles

4.12.10.3	**ASIC performance characterization** -- Functional tests shall be performed with simultaneous digital, analog and mixed signal circuitry to assess interactions, as well as, separate tests on each portion of the ASIC.
4.12.10.4	**Use of behavioral models** -- ASIC design shall develop behavioral and hardware description models to capture implementation of system design specifications and evaluate performance.
4.12.10.5	**Validation of behavioral models** -- Test vectors shall be developed and simulations performed to demonstrate the hardware description model design matches behavioral model, the gate level model matches the behavioral model, and fault containment is understood.
5	**SOFTWARE --** Software classified as mission-critical shall be designed to the relevant principles in section 4.11, ŅFlight Software System Design.Ó
6	**MANAGED MARGINS**
6.1	**Project Programmatic Resource Margins**
6.1.1	**Budget Reserve**
6.1.1.1	**Budget reserves at key project life cycle milestones --** Projects shall have budget reserves at key project life cycle milestones as indicated in Table 6.1.1-1
6.1.2	**Schedule Margin**
6.1.2.1	**Schedule margin at key project life cycle milestones Ń** Projects shall have schedule margin at key project life cycle milestones as indicated in Table 6.1.2 Š1.
6.3	**Flight System Development Resource Margins**
6.3.1	**General**
6.3.1.1	**Technical Margins** -- The design of flight systems shall include ample technical margins at the outset to be able to complete the development with acceptable residual risk to the mission.
6.3.2	**System Mass**
6.3.2.1	**Mass margin at key project life cycle milestones** -- Experience indicates there will likely be significant growth to deal with knowns and unknowns. Hence, Spacecraft system level mass margin shall be at least 30% at the PMSR, 20% at Project PDR, 10% at CDR, 5% at ATLO Readiness (ARR) and 2% at launch or as set by the project manager.
6.3.2.2	**Mass margin definitions** -- The below margin definitions shall be used by all projects in both formulation and implementation phases. Definitions: Margin = Allocation-- Current Best Estimate (CBE); % Margin = (margin/allocation) * 100
6.3.2.3.	**Mass margin status** -- Mass CBEs and mass growth shall be reported and compared with the required margin curves to assess margin status periodically (at least quarterly) and at implementation design reviews. Monthly mass reporting shall be considered, where appropriate.

Solutions - Reporting Process

- Standard Monthly Management Review process was neither sufficient or penetrating
- Created new **weekly** reporting process
  - Inputs and issues from each lower unit (subsystem level), system engineering level, and intermediate management levels
  - Reporting by each lower unit lead - - - "get it from the horse's mouth and ask your questions"
  - Highly metrics driven and reported metrics change with the work phase
  - Included a coherent list of work to go at the unit level and progress indicators - - - aka, the "punch list"
  - Assign action items and follow up on them the very next week
  - Identify new risks for the risk list
- All areas participated!
  - Engineering team, business team, science team, management team

Solutions - Review Process

- Followed the detailed review guidelines that contain scope and content for each required review
  - No more "winging it"
  - It's a lot of work, but if you are going to do it, do it right
- Ensured the independent review board membership and makeup was appropriate for the review being conducted
- Allocated sufficient preparation time and kept it in front of everyone
  - Don't succumb to the inevitable whining about being too busy with day-to-day issues
- At the conclusion of the review:
  - Ensured all issues were captured in writing and understood
  - Ensured each issue had associated action(s), assignee, and due date
  - Checked status weekly to ensure actions rapidly resolved
- For final issue closure, closed the loop with the review board member who generated the issue or action

Solutions - Teaming Arrangements

- Replaced most of the 1st and 2nd tier management team
- Organized product teams to take advantage of flight project experience and specific product knowledge
  - Combined membership from JPL and contractor
  - Only one person ultimately responsible for each subsystem
- Provided continuous management and engineering presence at the contractor site
  - Improved communications, continuous interaction
  - Quickly identify and resolve problems
  - Knowledge transfer
- Hands-on, day-to-day management by the Project Manager and Deputy Project Manager
- Weekly status review meeting served to keep team focused and everyone on the same page

Solutions - Flight System V&V Process

- Implemented “Test as fly and fly as you test” philosophy and process to define test program and content at the system level
  - If you test it this way, then fly it that way. If you are going to fly it in a certain way, then test it that way
  - Exceptions are inevitable, but why are the exceptions OK and how can the risk be mitigated?
  - Similar to Flight Project Practices and Design Principles Process
- Defined and generated an Incompressible Test List
  - Recognizing unforgiving launch and encounter windows, this list defined the tests that must be completed prior to launch or prior to encounter
  - Completion means **all** data analyzed and **all** issues resolved, fixed, and re-tested
  - Provided priorities and focus on what needed to be done
  - Expended significant effort on increasing test bed fidelity and validating test bed models
- Additional staff brought on to define and implement the data reduction and analysis capability

Example - Test as You Fly, Fly as You Test

Cat'y	V&V Activity	Nomin Off-Nc	Venue	Tes Typ	H/W Conf	V&V Operation	Description	Test as you Fly Exceptions
I-20	HGAG unlatch and full range of motion	Nom	FB	I&T	A	Use HGAG Checkout MST	HGA Gimbal deployment using flight checkout sequence (ir motion/interference checks)	HGA was not installed. Operation of the HGA gimbal with th possible but discouraged. Full range of motion testing of gir to verify no interference with harnesses and blankets. Interf
I-21	S-Band Cross Link	Nom	FS	I&T	A&B	Impactor Checkout and Standalone I&T Test	Demonstrated S-band RF link compatibility (not just hard lin Airlink RF verified via "parasitic" test antenna on Flyby while by analysis.	For separated spacecraft configuration RF was verified in h via RF probe in mated configuration. Antenna properties we

Example - Incompressible Test List

Cat'y	V&V Activity	Nominal Off-Nom	Venue	Test Type	H/W Config	V&V Operation	Description
I-1	Launch Vibration	Nom	FS	I&T	A	Flight System Vibration Test	EDVP (Proto-flight level), 3-axis. Configured and powered to prelaunch confi
I-2	Launch Acoustics	Nom	FS	I&T	A	Flight System Acoustic Test	EDVP (Proto-flight level). Configured and powered to prelaunch configuration
I-3	Flyby/Impactor Mechanical/Electrical Sep and Pyroshock	Nom	FS	I&T	A&B	Separation/Pyro Test	Includes Flyby/Impactor pyro device separation and electrical disconnect. Pl configuration. Also serves as final pyroshock environment verification.
I-4	EMI/EMC	Nom	FS	I&T	A	EMI/EMC (Includes Seq Fragments Impactor C/O)	Separation (into fuses), RCS/TCM (with ACC loads), Encounter imaging (per Impactor Checkout & thruster ops(with ACC loads)
I-5	FS Thermal Vacuum/Balance	Nom	FS	I&T	A&B	Flight System Thermal Vac/Balance	Per Test plan; pre-launch configuration @ pump down; High power operation
I-6	Impactor Thermal Vacuum/Balance	Nom	FS	I&T	A&B	Impactor Thermal Vac/Balance	Per Test plan; post separation encounter configuration
I-7	Flyby Mass Properties/Balance	Nom	FB	I&T	n/a	FB Mass Props	Required to obtain cg and inertia for ADCS. Performed dry @ BATC
I-8	Impactor Mass Properties/Balance	Nom	Imp	I&T	n/a	Impactor Mass Props	Required to obtain cg and inertia for ADCS. Performed dry @ BATC
I-9	FS Mass Props/Final Balance, Launch Config	Nom	FS	I&T	n/a	FS Mass Properties @ KSC	Balance Wet @ KSC using Oscillating Balance Machine

Solutions - Effective Risk Management

- Established simple but effective Risk Management Process
  - Generated spreadsheet based Risk List - - a living document
  - Active, Accepted and Retired risks
  - Review risks frequently, assign actions and follow-up on those actions
  - All project areas attend these Risk List reviews
  - Assign risk rating to each risk and change as the risk is mitigated or worsens
  - The value of the rating process is in the discussion it engenders and the tremendous increase in understanding/characterization of the risk

“Rigor, penetration, and follow-up”

Active Risks

	1	2	3	4	5
5	1		1		
4		1			
3					
2	1	2		3	2
1		1	2	4	

Consequence

Likelihood	
1	Very low - Very unlikely
2	Low - Unlikely
3	Moderate - Significant likelihood
4	High - More likely than not
5	Very high - Almost certain

Consequence	
1	Minimal or no impact to mission
2	Small reduction in mission return
3	Cannot meet full mission success
4	Cannot meet minimum mission success
5	Mission catastrophic - no data returned

Example Risk List

Ref No	Risk Rating	Risk Item	Impact Details	Consequence	Likelihd	Initiator	Originat Date	Risk Typ	Resp. S/S Actionee	Mitigation Actions	Comments
48		RAD750 performance (I software) may not be ad support minimum scienc the Flyby during encoun bottlenecks are resulting images. Blocks of dropp time of impact would vio		3	1			D	Patel	1) Tiger Team formed to find dropped images 2) Root cause determined to insufficient number of buffers 3) Solution implemented - turn software function in file system enough buffers with some mar	See Tiger Team report: Dropp Team Report, from G. Reeves Distribution, 8 November 2004 This risk was reopened in Feb evaluation. Risk Rating is from assessments. In work.
88		HGA Gimbal Disturbanc high.	Disturbance torques may to smear.	2	2			M	J. Stober	Test for Disturbance torques e phase and modify encounter s the-moment Part of the Cruise timeline. The designed with the support of th Instrument, and ADCS engine	Smoothed control algorithm wa tested in HGA jitter test. Results being e
124		Cosmic Ray during enco 'spoof' AutoNav, causing miss comet.		4	2	J. Wonsever	December-08	M	D. Kubitschek	EWG is reviewing in-flight data MRI instruments to determine case environment. Will then p determine margins.	Update based on results of EW
127		HRI LUT is causing image corruption		3	1	R. Grammier	February-09		D. Hampton	Upload new versions of the IR Ops Procedure) to use the cor uncompressed data.	MCR has been submitted to co
129		Fault Protection thresho set properly for all missio causing unintended resp		2	2	R. Grammier	February-09		G. Roat K. Patel	Review team is reevaluating th persistance values for cruise c spacecraft health and safety, r the FP objective.	The review team consists of FP subsystem, and a cognizant su from other JPL flight programs Roat - Cruise parameter review Patel - Encounter parameter re
125a		HRI out of focus - impac sequences and Level 1 r	Refer to "Deep Impact H Impacts on Engineering Requirements" slide pac 3/30/05. Will update based on decisions.	3	5				A'Hearn	Engineering/Autonav will use t Flyby. HRI will become a back that MRI fails. Flyby closest a will remain the same. Some a Impactor and Flyby automat s to account for use of	We need an update of the pac Weinberg and Hampton that p Science and engineering requi package should be updated to decisions made under mitigatio [Grammier to fwd updated pkg

Solutions - Effective Risk Management

- All solutions and processes feed the Risk Management Process

Solutions - Effective Risk Management

- Conducted several, in-depth, risk reviews
  - Risk Review for each mission phase (five)
  - Two Project level risk reviews pre-launch
  - Three Project level risk reviews for encounter
- Example Risk Review Agenda on next two slides

Risk Review Agenda

1.0 Project Overview/Status …………………………………………………………………………………	Rick Grammier
2.0 Flight Project Practices and Design Principles Compliance Status & Exceptions……………	Rick Grammier
3.0 Risk Issues Status:	
3.a Design Verification (test, analysis, inspection)…………………………………………………..	Carl Buck
3.b Functional and Environmental Verification ………………………………………………………	Carl Buck
3.c Red Flag PFRs, Significant PFRs and TAWs ……………………………………………………	Tim Larson
3.d Waivers & Waivers with Dissent SPF List ………………………………………………………..	Tim Larson
3.e Open Flags & IRs …………………………………………………………………………………..	Tim Larson
3.f Pending hardware design changes and impacts ………………………………………………..	Keyur Patel
3.g Pending software design changes and impact …………………………………………………	Anne Elson
3.h Pending flight sequence design changes ……………………………………………………….	Dave Spencer
3.I Total operating hours/failure-free operating hours ……………………………………………	Tim Larson
3.j Open Action items (from HRCRs, Reviews, etc.) ………………………………………………..	Rick Grammier
3.k Safety issues ………(Not to be Presented)……………………………………………………..	Tim Larson
3.l Parts Issue …………………………………………………………………………………………	Tim Larson
3.m Model Status (ADCS, Thermal, Power, Propulsion) ……………………………………………	Keyur Patel
3.n Exceptions to “test as you fly” / “fly as you test” ………………………………………………	Carl Buck
3.o Test bed fidelity shortfalls/differences and status …………………………………………….	Keyur Patel
3.p Limited Life Items / Consumables ………………………………………………………………….	Tim Larson
4.0 Status of Incompressible Test List Verifications …………………………………………………	Carl Buck
5.0 End-To-End Tests and Results/Issues (MRT, CTT) ……………………………………………….	Carl Buck
6.0 Status of IV&V Issues ………………………………………………………………………………	Anne Elson

Agenda (Continued)

7.0 Mission Operations Risk Issues ………………………………………………………………….. Dave Spencer

7.a Procedures, contingency plans, flight rules, cmd/tlm, dictionaries, etc

7.b Training Plans

7.c Staffing Plans

7.d Flight Operating Margins

8.0 Operations Status …………………………………………………………………………….. Dave Spencer

9.0 MAM Risk Assessment …………………………………………………………………………. Tim Larson

10.0 Project Risk Summary, Including Residual Risk (Technical and Programmatic) ………….. Rick Grammier

11.0 Conclusion / Open Items / Plans ………………………………………………………………….. Rick Grammier

State of Project at Launch

- Encounter related ITL not completed
  - Particularly faulted encounter tests
- Several open issues related to encounter design
- Encounter contingency plans not identified, developed or tested
- Still had test bed fidelity issues to resolve for encounter testing
- Operations team certified/trained, but still green
- Practically every day of 6 month journey to Tempel 1 required spacecraft and test bed activity
- Low risk posture for launch and initial checkout
- Medium to high risk posture for “cruise” and encounter

⇒ Significant engineering, development and test of encounter software, sequences and fault protection still required

⇒ Too much work remaining for current size of operations team

Solutions (Post Launch)

- Retained majority of development team remaining at launch
- Retained processes used so successfully to get to launch
  - Weekly status report, punch lists, risk reviews, etc.
- Formed Encounter Working Group (EWG) to complete development and V&V of encounter
  - Firewall between EWG and daily spacecraft operations team
  - Activity led by deputy PM
  - Formed an Encounter Red Team to follow and challenge the Project regarding encounter design and verification
- Pretty much 24/7 operation after launch

Encounter Risk Management

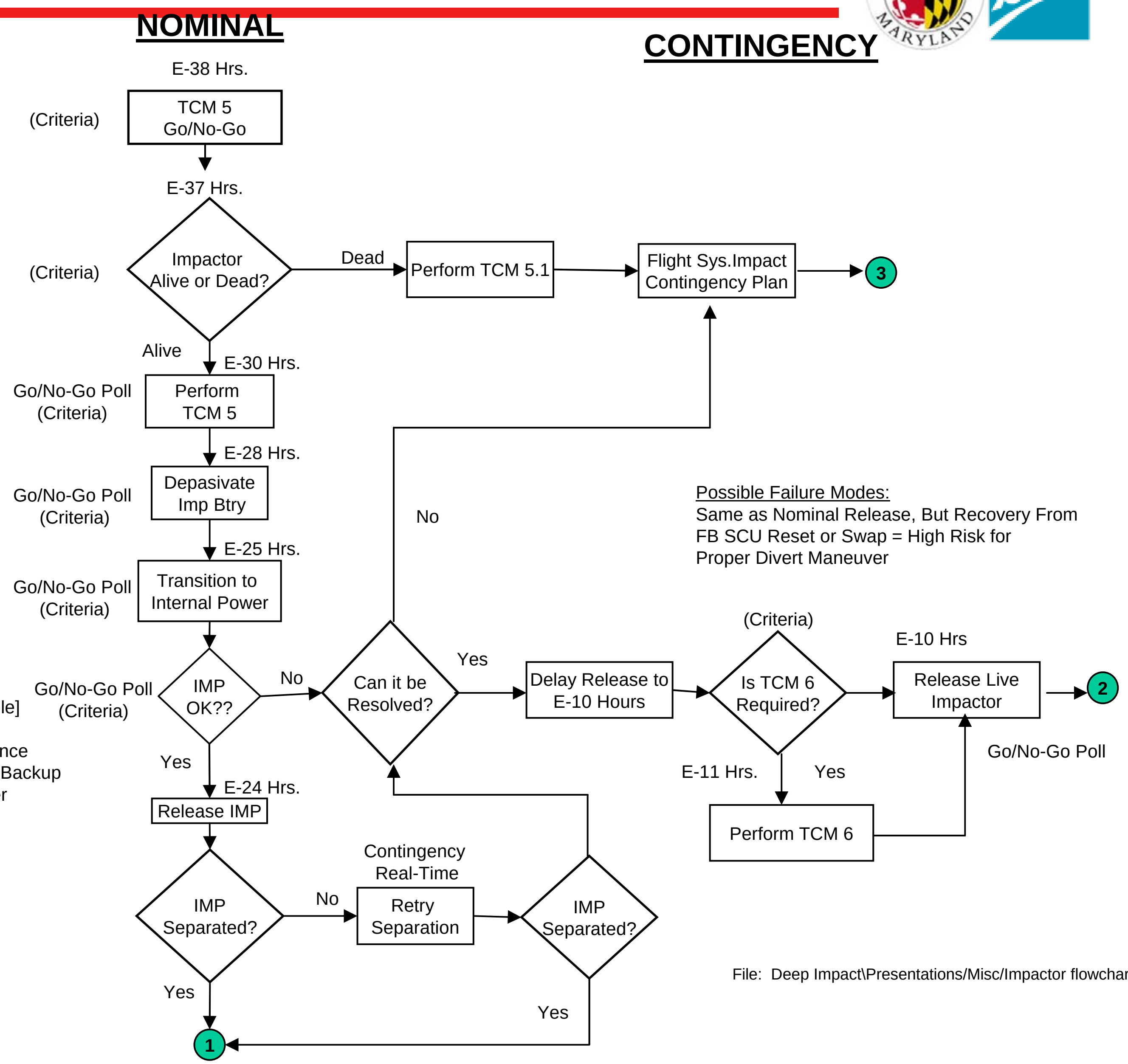
- Accurate tracking and closure of all encounter related open items at time of launch
- 3 sigma and 6 sigma testing of encounter sequences
  - Understand what parameters we were most sensitive to
- Generation of encounter decision tree
- Identification of required encounter contingencies
  - Generation and V&V of same
- Conducted several encounter operational readiness tests (ORTs), under both nominal and faulted conditions
- Incorporated changes due to in-flight behavior
  - High Resolution Instrument (HRI) de-focus
  - Star tracker performance
- In flight tests to reduce “first time in flight” items
- Conducted three encounter risk reviews with the Red Team and senior management
- As time started to run out, concentrated more on testing nominal encounter vs. faulted encounter

Encounter Decision Tree

1) Imp = Single String
2) Complete Imp Check-out At E-9 Days And Leave On
3) Any Failure Except S-band = Dead Impactor
4) Probability @ This Point = Negligible

1) Probability of Imp Failure Due to TCM-5 = Negligible
2) Going to Impactor Internal Power = Most Likely Failure at this Point (1st in Flight) → Probability = Low to Negligible

Possible Failure Modes:
Failed Electrical Separation (1st in Flt.) [Low]
Failed Mechanical Separation (1st in Flt) [Low]
Failed Thrusters Post-Sep. (1st in Flt.) [Low to Negligible]
SCU Reset @ Separation (Flyby or Imp) [Low]
- Imp = FP Recovers & Resumes Critical Sequence
- FB = FP Recovers on Same Side or Swaps to Backup if HW Failure = Possible Failed Divert ⇒ Larger Divert Trim Maneuver (i.e., Recoverable)

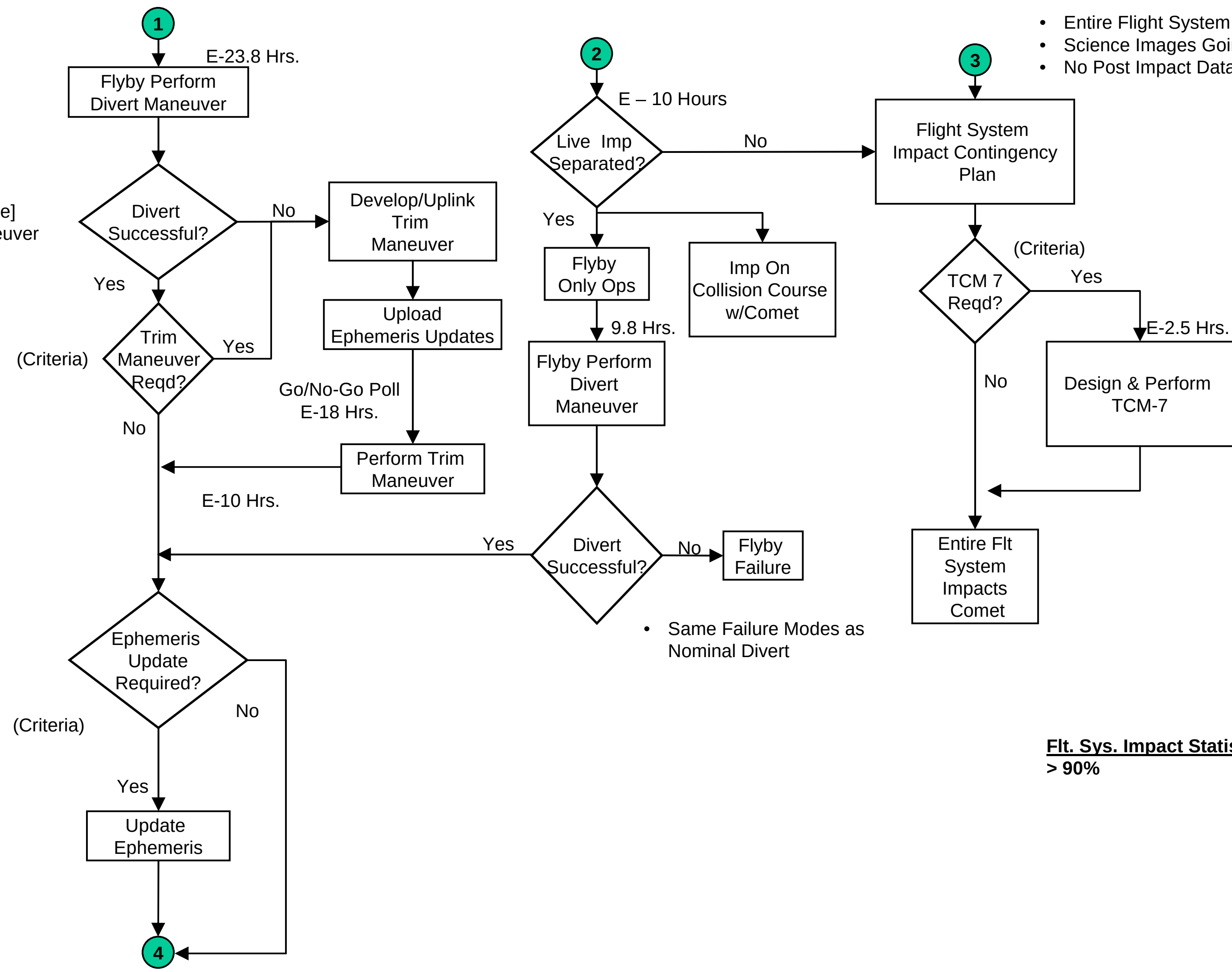


File: Deep Impact\Presentations/Misc/Impactor flowchart 3-05

Page 2

Encounter Decision Tree

NOMINAL | CONTINGENCY



- Entire Flight System Impact
- Science Images Going In
- No Post Impact Data

<u>Possible Failure Modes:</u>

- HW Fault Causes FP to Interrupt Burn, Recover & Resume [Negligible] This is Recoverable with Trim Maneuver
- SW or Sequence Error Results in Under Burn or Over Burn [Low]

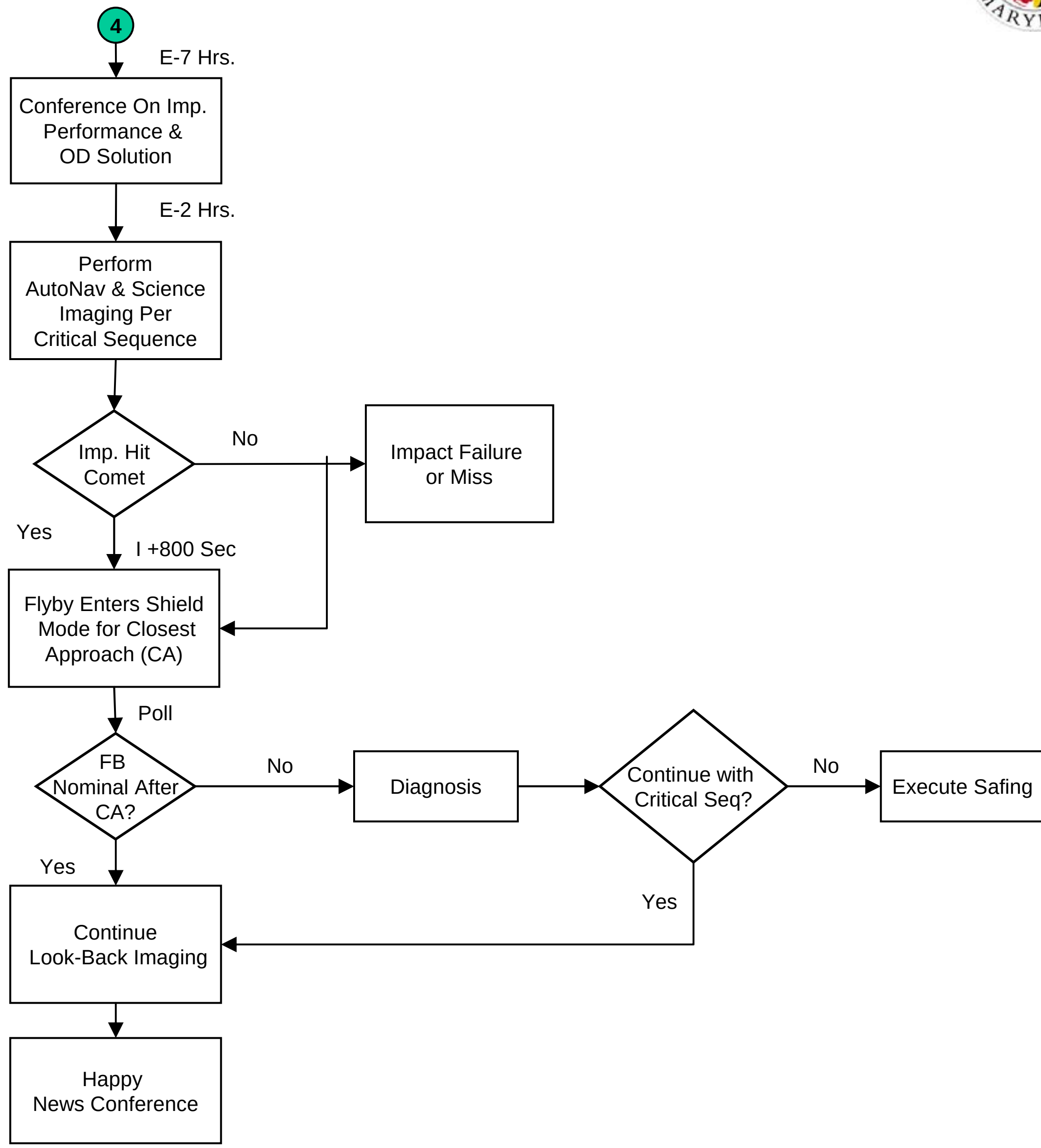
Nominal Impact Statistics
Miss - 0.067%
Dark - 0.10%
Lit Impact - 99.83%

<u>Flt. Sys. Impact Statistics</u>
> 90%

NOMINAL

(Criteria)

Possible Failure Modes:
- Incorrect FP Enable/Disable Settings [Low]
- AutoNav Spoof by Cosmic Rays [Low]
- Solar Flare [Low to Medium]
- S-Band Failure [Low]
- Particle Hits on Flyby at Closest Approach [Low]
- Hot Pixels Form in MRI or ITS Center of CCD Area = AutoNav Failure [Low]
- HRI or MRI Failure [Negligible]



Enough Said!